PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-121387
(43)Date of publication of application : 06.05.1997

(51)Int.Cl. H04Q 7/38
H04Q 7/34

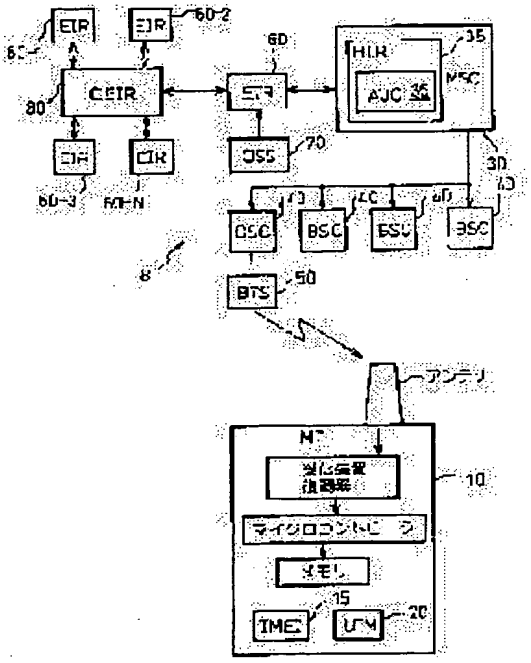
(21)Application number : 08-204957
(22)Date of filing : 02.08.1996

(71)Applicant : NOKIA MOBILE PHONES LTD
(72)Inventor : MECHE PAUL S
VAISANEN AHTI

(30)Priority
Priority number : 95 511519 Priority date : 04.08.1995 Priority country : US

(54) MOBILE COMMUNICATION NETWORK AND METHOD FOR LOCKING REMOTE MOBILE TERMINAL EQUIPMENT SELECTED FROM THE MOBILE COMMUNICATION NETWORK

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the mobile means network in which a lock function of a user identification module(UIM) is automatically started by a signaling of a communication network via a common radio interface from a base station to a mobile telephone set.
SOLUTION: The communication network 8 inquires of an international mobile terminal identification(IMEI) unit 15 of a mobile telephone set 10 used by a subscriber of the system periodically or regularly. If the IMEI of the mobile telephone set is listed on a 'theft article list', the communication network communicates a message with the mobile telephone set via a radio interface and allows the mobile telephone set to start a UMI lock function 20 based on the sent bit pattern.



LEGAL STATUS

[Date of request for examination] 01.08.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－121387

(43)公開日　平成９年(1997)５月６日

(51)Int.Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｑ　7/38			Ｈ０４Ｂ　7/26	１０９Ｓ	
7/34			Ｈ０４Ｑ　7/04	Ｃ	

審査請求　未請求　請求項の数18　ＯＬ　（全 12 頁）

(21)出願番号　特願平8－204957

(22)出願日　平成８年(1996)８月２日

(31)優先権主張番号　５１１５１９

(32)優先日　1995年８月４日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　590005612
ノキア　モービル　フォーンズ　リミティド
フィンランド国、エフアイエヌ－24101　サロ、ピー．オー．ボックス　86、ナコランカツ　8

(72)発明者　ポール　エス．メシェ
アメリカ合衆国，テキサス　75082，リチャードソン，スプリング　レイク　ドライブ　2618

(72)発明者　アーティ　パイサネン
アメリカ合衆国，カリフォルニア　92014，デルマー，マンゴー　ドライブ　13353

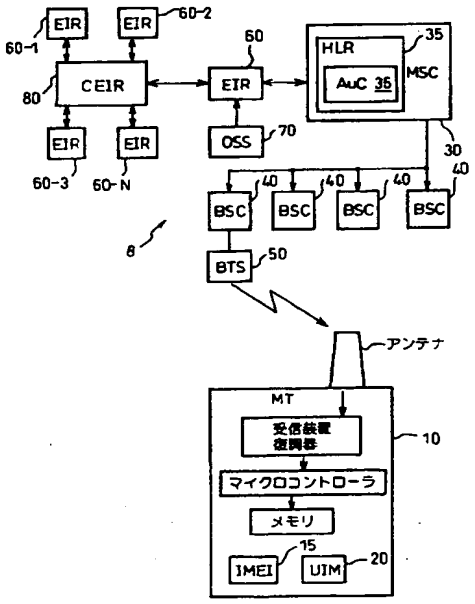
(74)代理人　弁理士　石田　敬　（外３名）

(54)【発明の名称】　移動通信網及び該移動通信網の選択された遠隔移動端末装置をロックする方法

(57)【要約】

【課題】　基地局から移動電話への共通無線インターフェースを介する当該通信網のシグナリングによってユーザー識別モジュール（ＵＩＭ）のロック機能が自動的に起動されるようになっている移動通信網を提供することを目的とする。

【解決手段】　該通信網は、該システムで加入者が使っている移動電話の国際移動端末装置識別（ＩＭＥＩ）ユニットを定期的に又は規則的に問い合わせる。もし移動電話のＩＭＥＩが「盗品リスト」に載っていたならば、該通信網は、無線インターフェースを介して該移動電話とメッセージをやりとりして、送ったビットパターンにより該移動局にＵＩＭロック機能を起動するように指令する。



1　　2

【特許請求の範囲】

【請求項1】　少なくとも1つの中央基地交換網と、電子信号を送受信するための回路を内蔵する複数の遠隔移動端末装置とから成る移動通信網において、前記遠隔移動端末装置の各々は、該装置からの送信を制御するための特定のユーザー専用のデータを内蔵するユーザー識別モジュール（ＵＩＭ）を含んでおり、

前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の選択された遠隔移動端末装置を前記の含まれているＵＩＭに選択的にロックするとともに前記の含まれているＵＩＭを前記の選択された遠隔移動端末装置にロックするための手段を含んでおり、これにより前記の選択された遠隔移動端末装置の他の前記ＵＩＭでの動作を選択的に阻止するとともに前記の含まれているＵＩＭの他の前記遠隔移動端末装置での動作を阻止することを特徴とする移動通信網。

【請求項2】　前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の選択された遠隔移動端末装置を前記の含まれているＵＩＭにロックすることにより前記の選択された遠隔移動端末装置の他の前記ＵＩＭでの動作を阻止するための手段を有する、請求項1に記載の移動通信網。

【請求項3】　前記中央基地交換網は、選択された遠隔移動端末装置にデータ信号を送って前記の含まれているＵＩＭを前記の選択された遠隔移動端末装置にロックすることにより前記の含まれているＵＩＭの他の前記遠隔移動端末装置での動作を阻止するための手段を有する、請求項1に記載の移動通信網。

【請求項4】　前記遠隔移動端末装置の各々の各ＵＩＭは前記の特定のユーザー専用のデータを記憶するための記憶手段を含んでいる、請求項1に記載の移動通信網。

【請求項5】　前記遠隔移動端末装置の各々の各ＵＩＭは、前記中央基地交換網から送られた前記データ信号に応答して、その送られたデータ信号のデータが前記遠隔移動端末装置の前記ＵＩＭに記憶されている前記の特定ユーザー専用のデータと同一であるときには前記遠隔移動端末装置の他のＵＩＭでの動作を阻止するための手段を含む、請求項1に記載の移動通信網。

【請求項6】　前記遠隔移動端末装置はセルラー電話である、請求項1に記載の移動通信網。

【請求項7】　前記遠隔移動端末装置の各々は独特の国際移動端末装置識別（ＩＭＥＩ）ユニットを含む、請求項1に記載の移動通信網。

【請求項8】　前記中央基地交換網は、少なくとも1つの基地局コントローラ（ＢＳＣ）と、前記データ信号を前記の選択された遠隔移動端末装置に送るための少なくとも1つの基地局送受信システム（ＢＴＳ）とに接続された移動交換センター（ＭＳＣ）を含む移動交換網を含む、請求項1に記載の移動通信網。

【請求項9】　前記移動交換センター（ＭＳＣ）は、真実性の確認センター（ＡＵＣ）を有するホームロケーション・レジスタ（ＨＬＲ）を含んでおり、前記移動交換センター（ＭＳＣ）は、前記移動端末装置の正当性及び状況に関するデータを内蔵する装置識別レジスタ（ＥＩＲ）に接続されている、請求項8に記載の移動通信網。

【請求項10】　少なくとも1つの中央基地交換網と、電子信号を送受信するための回路を内蔵する複数の遠隔移動端末装置とを有する移動通信網の選択された遠隔移動端末装置をロックする方法において、前記遠隔移動端末装置の各々は、該装置からの送信を制御するための特定のユーザー専用のデータを内蔵するユーザー識別モジュール（ＵＩＭ）を含んでおり、この方法は、

前記中央基地交換網から選択された遠隔移動端末装置のＵＩＭへデータ信号を送るステップ（ステップ1）と、前記中央基地交換網から送られた前記データ信号を受け取って前記の選択された遠隔移動端末装置を前記の含まれているＵＩＭに選択的にロックし且つ前記の含まれているＵＩＭを前記の選択された遠隔移動端末装置にロックすることにより、前記の選択された遠隔移動端末装置の他のＵＩＭでの動作を阻止するとともに前記の含まれているＵＩＭの他の前記遠隔移動端末装置での動作を阻止するステップ（ステップ2）とから成ることを特徴とする方法。

【請求項11】　前記の含まれているＵＩＭは前記の特定の遠隔移動端末装置にロックされる、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項12】　前記のステップ2において前記の特定の遠隔移動端末装置は前記の含まれているＵＩＭにロックされる、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項13】　前記のステップ2は、前記ＵＩＭの前記の特定ユーザー専用データを前記中央基地交換網から受け取ったデータ信号と比較し、前記ＵＩＭをロックし、前記の受け取ったデータが前記の特定ユーザー専用データと同一であるときには前記の選択された遠隔モジュールの動作を阻止することを含む、請求項10に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項14】　前記ＵＩＭに内蔵された真実性の確認手続きを更に含んでおり、前記のステップ2は前記真実性の確認手続きの結果を比較することを更に含む、請求項13に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項15】　前記のステップ1は、前記の選択された移動端末装置の国際移動端末装置識別（ＩＭＥＩ）情報を得、国際移動端末装置識別情報の状況に関して装置識別レジスタ（ＥＩＲ）に問い合わせて、その選択された遠隔移動端末装置が盗まれているか否か判定し、ユーザー識別モジュールロックコマンドを前記の選択された

遠隔移動端末装置に送るステップを更に含む、請求項１０に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項１６】　選択された遠隔移動端末装置の前記ＵＩＭに内蔵されている真実性の確認手続きを更に含んでおり、前記のステップ２は前記真実性の確認手続きの結果を比較することを更に含む、請求項１５に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項１７】　前記のステップ２は前記中央基地交換網から送信された受信コマンドがロックコマンドであるか否か判定し、前記ロックコマンドの真実性を確かめ、移動端末装置のユーザー識別モジュールへのロックを実行するステップを含む、請求項１０に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【請求項１８】　前記のステップ２は、前記の選択された遠隔移動端末装置がロックされたという肯定応答を前記の選択された遠隔移動端末装置から前記中央基地交換網へ送るステップを更に含む、請求項１７に記載の移動通信網の選択された遠隔移動端末装置をロックする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば携帯電話などの通信用移動端末装置と、その様な端末装置を利用する通信網とに関する。本発明は、特に、ユーザー識別モジュール（ＵＩＭ）を採用する携帯電話に関する。

【０００２】

【従来の技術】電話を手操作でユーザー識別モジュール（ＵＩＭ）にロックすることのできる加入者又はユーザー識別装置を持った携帯電話システムが知られている。

【０００３】１９９３年３月２９日に出願された「移動端末装置の加入者識別モジュールを遠隔操作で更新する機能を持った移動通信網」という題名の、グリーン（Green）の欧州特許出願第９３３０２４２０．０号（公報第０５６２８９０Ａ１号）は、無線電話で移動電話と通信をする移動交換センターを含む交換網を有する通信網を開示している。その移動装置は、移動装置の動作と、移動装置のユーザーが利用し得る設備とを制御するためのデータを記憶する加入者識別モジュールを内蔵している。交換網は、加入者識別モジュールに記憶されているデータを変更し、従って、利用可能な設備での動作を変更する更新信号を移動装置に送る。

【０００４】前記の出願は、無線でＵＩＭをプログラミングする技術を開示しているが、公報第０５６２８９０Ａ１に記載されているように電話をプログラミングする方法や技術を開示してはいない。

【０００５】

【発明が解決しようとする課題】目下、特にＧＳＭ（the Groupe Speciale Mobile）規格に基づく移動電話は、

以前は加入者識別モジュール又はＳＩＭと称せられ、現在はユーザー識別モジュール（ＵＩＭ）と称せられている電子モジュールを内蔵している。このＵＩＭは移動電話（本明細書では移動端末装置（ＭＴと略記）とも称する）により使用されるべきデータを記憶する。ＵＩＭは、特定のユーザーのための独自の識別子を持つように予め構成されるとともに、適当な真実性の確認機能を持つこともできる。ＵＩＭは、ページングメッセージや電話番号簿などの暫定的データを記憶することもできる。

【０００６】現在のＧＳＭに基づくシステムでは、加入者識別は移動端末装置（ＭＴ）には関連していない。それは、ＵＩＭのユーザーによりなされる。ＵＩＭは、電話に取り付けられるようになっていて独自のユーザー識別情報を有するモジュール或いはスマートなカードである。

【０００７】ＧＳＭに基づくシステムでは、ユーザーは自分のＵＩＭカードをどの移動端末装置にも挿入することができ、使用されているその特定の端末装置に付随する情報ではなくてそのＵＩＭ上の情報を介してＧＳＭ通信網により認識される。このシステムでは、移動端末装置はＩＭＥＩ（International Mobile Equipment Identity （国際移動端末装置識別）情報）により識別可能である。しかし、この情報をチェックするための照会は、処理に関して「費用がかかり」、通常は呼毎には確認されない。

【０００８】これらの要素を、ＧＳＭに基づくインターフェースを使用する端末装置の広大な「ブラックマーケット」を開拓した泥棒達が活用して、数十万台もの移動端末装置が毎年盗まれるという結果を招いている。

【０００９】

【課題を解決するための手段】本発明は、盗まれた移動端末装置を発見したならば、その移動端末装置を、その移動端末装置で使用されているＵＩＭカードに直ちに「ロック」することによって、その盗まれた移動端末装置の価値を低下させるものである。移動端末装置を特定のＵＩＭにロックするということは、その移動端末装置を他のＵＩＭで使用することができなくなるということを意味し、従ってその再販価格を低下させる。また、この操作に加えて、関係当局によるその移動端末装置の取り戻しのための追跡調査のために、盗まれた移動端末装置に使われているＵＩＭに関する情報収集を行う。

【００１０】一般に、ロック機能は４～８桁のピンコードを有し、起動される場合には、移動端末装置がパワーアップされる毎に、いずれかの操作が行われる前に、入力されなければならない。

【００１１】また、移動端末装置は、マスターパスワード無しでは無許可のＵＩＭを移動端末装置が受け入れるのを阻止する様に設計されたＵＩＭロックも提供する。起動されると、移動局は前に許可されたＵＩＭだけを受け入れる。

【００１２】本発明の目的は、ＵＩＭのロックとロック解除とがＢＴＳと移動局との共通無線インターフェース経由のシグナリングを介して通信網により自動的に起動されるようになっている移動電話システムを提供することである。

【００１３】本発明の他の目的は、ＵＩＭを、それと関連する特別の移動電話にのみ使用し得るようにＵＩＭをその移動電話に随意にロックすることができるようになっている移動電話システムを提供することである。

【００１４】本発明の他の目的は、移動電話を特別のＵＩＭにのみ使用し得るように移動電話をそのＵＩＭに随意にロックすることができるようになっている移動電話システムを提供することである。

【００１５】本発明の他の特徴、長所及び利益は、添付図面と関連させて以下の記述を考慮することから明かとなろう。如上の一般的記述と以下の記述は例示的な説明をするものであって、本発明を限定するものではないことが理解されなければならない。本発明に組み込まれて本発明の一部を構成する添付図面は、明細書とともに、本発明の原理を一般的用語で説明するのに役立つものである。明細書及び図面の全体にわたって同じ数字は同じ部分を指している。

【００１６】

【発明の実施の形態】現在、ＧＳＭ移動端末装置は、もし正当な所有者が自分の移動端末装置を自分のＵＩＭに「ロック」することを忘れたり無視したりした場合には、盗難後に単に有効なＵＩＭカードを挿入するだけで簡単に再使用される。また、賃貸ユニットは通常は特別のＵＩＭカードにロックされていないので、賃貸の移動端末装置は特に窃盗に対して弱い。この様な事情があるために盗まれたＧＳＭ移動端末装置の繁盛している市場がある。本発明は、盗品であると判定された移動端末装置を該移動端末装置に挿入されているＵＩＭにロックすることにより再販売に関しての価値を低下させることのできるメカニズム及び方法を定義する。

【００１７】本発明の移動端末装置（ＭＴ）は、無線でのコマンド（over-the-air command）によりＵＩＭにロックされる。また、本発明は、移動端末装置に挿入されたＵＩＭをその移動端末装置のＩＭＥＩにロックすることによって、そのＵＩＭを、該ＵＩＭがロックされた移動端末装置においてのみ使用し得るようにすることのできるシステムを提供する。

【００１８】詳しく述べると、電話通信網は、該システムで加入者が使っている移動端末装置のＩＭＥＩに定期的に又は規則的に照会をする。もし移動端末装置のＩＭＥＩが「盗品リスト」に載っているのが分かったならば、通信網は無線インターフェースを介して送信したビットパターンを用いてＵＩＭロック機能を起動するべき旨のメッセージを該移動端末装置とやりとりすることにより該移動端末装置にＵＩＭロック機能を起動するように指令する。

【００１９】通信網は、通常、例えば無線電話等により移動電話等の移動端末装置（ＭＴ）と通信をする移動交換センター（ＭＳＣ）を含む。移動端末装置は、該移動端末装置の動作と、そのユーザーが利用することのできる設備とを制御するためのデータを記憶する加入者（又はユーザー）識別モジュールを内蔵する。

【００２０】本発明によると、交換網は、移動端末装置のデータ及び保障状況及び／又はユーザー識別モジュールの保障状況を変更する更新信号を移動端末装置に送る。

【００２１】図１に通信網が示されており、この通信網は移動電話等の移動端末装置（ＭＴ）１０と交換網８とを含む。交換網８は、移動交換センター（ＭＳＣ）３０と、移動端末装置１０がその中で動作することのできる種々のセルサイトのための複数個の基地局コントローラ（ＢＳＣ）４０とを含む。装置識別レジスタ（ＥＩＲ）６０は共通装置識別レジスタ（ＣＥＩＲ）８０に接続されており、このＣＥＩＲ８０は他の交換網とそれに関連する移動端末装置とに関連する他の装置識別レジスタ６０－１、６０－２、…６０－Ｎに接続されることができる。装置識別レジスタ６０を更新するためのオペレーションサブシステム（ＯＳＳ）７０を設けることができる。移動端末装置１０等の移動端末装置との無線での通信は基地局送受信ユニット（ＢＴＳ）５０を介して行われる。

【００２２】通信網の移動端末装置１０等の各端末装置は、特定のユーザーのための独特の予めプログラムされたデータを記憶するユーザー識別モジュール（ＵＩＭ）２０と、国際移動端末装置識別（ＩＭＥＩ）ユニット１５とを有する。各国際移動端末装置識別ユニット１５は、その移動端末装置１０に独特のものであって、移動交換センター３０に対して移動端末装置１０を特定するために使用される。

【００２３】図１において、多数の基地局コントローラＢＳＣ４０のうちの１つを介して、それに付随する基地局送受信システムＢＴＳ５０経由でＭＳＣ３０から移動電話又はその他の移動端末装置ＭＴ１０へ通常の通信が通信ネットワーク間で行われる。

【００２４】ＭＴ１０は、ユーザー識別モジュール（ＵＩＭ）２０をそなえ、該モジュールは特定のユーザーの独特の識別子と、そのユーザーが利用することのできる真実性の確認機能とを記憶する。ＭＴ１０は、独特の国際移動端末装置識別（ＩＭＥＩ）ユニット１５も内蔵している。

【００２５】ＭＳＣ３０は、特定のユーザーのためのホームロケーション・レジスタＨＬＲ３５にアクセスするための通信チャネルを有する。ＨＬＲ３５は、ユーザーの真実性確認のために使われる保障データを管理する真実性確認センターＡｕＣ３６と呼ばれる機能部分を含ん

でいる。ＨＬＲ３５のＡｕＣ３６の機能と、ＵＩＭ２０の対応する真実性確認機能とは、連携して、ユーザーを確認することにより種々の不正使用を防止するための比較的に確実で強固な手段を提供するものである。

【００２６】ＭＳＣ３０は、通信網に知られている国際移動端末装置識別（ＩＭＥＩ）ユニット１５を介して移動端末装置ＭＴ１０の正当性及び状況に関する情報を内蔵するデータベースである装置識別レジスタＥＩＲ６０にアクセスするための通信チャネルを有する。　ＥＩＲ６０は３つの「リスト」を内蔵している。１つは、有効な種類承認済み移動端末装置ＭＴ１０の範囲を包含する「ホワイトリスト」である。他の１つは、盗まれたか、或いはひどく故障していると通知されているＩＭＥＩ１５のリストを包含する「ブラックリスト」である。第３のリストは、当局がブラックリストに載せるべきことを確かめる前の怪しい装置を含む、「ホワイト」と「ブラック」との中間の「グレイリスト」である。

【００２７】本発明のプロセスのステップは図２及び図３のブロックで示されているとおりである。ＭＴ１０とＭＳＣ３０との間での通信の開始の際に、当業者に周知されている種々の必須のメッセージのやりとりが行われる。この在来のメッセージのやりとりの後に、ＭＳＣ３０は、図２のブロック３００に示されているようにＭＴ１０のＩＭＥＩ１５を得るように求められる。在来のシステムでは、これは、ＭＴ１０への識別要求メッセージ（IDENTITY REQUEST Message）の送信により達成される。在来のＭＴ１０は、ＩＭＥＩ１５を含む識別応答メッセージ（IDENTITY RESPONSE Message)で答える。本発明の特徴の１つは、ＩＭＥＩ１５の情報を上記した在来の必須のメッセージに含ませることによって、このメッセージ交換を最適化することにある。

【００２８】本発明の好ましい実施例では、ＩＭＥＩ１５の情報はＭＴ１０からの位置更新要求メッセージ（LOCATION UPDATING REQUEST Message)に含まれる。

【００２９】在来のシステムにおける位置更新要求メッセージのフォーマット及び構造は、ＭＴ１０がＵＩＭ２０を内蔵していなかったり或いはＵＩＭ２０が何らかの理由から無効であると考えられる場合には、ＩＭＥＩを含むだけである。本発明の最適化の特徴の主題は、位置更新要求メッセージにＴＭＳＩ又はＩＭＳＩも含まれているか否かに関わらず、常にＩＭＥＩをこのメッセージに含ませることである。ＴＭＳＩ（Temporary Module Subscriber Identity）又はＩＭＳＩ（International Module Subscriber Identity）も位置更新要求メッセージに含まれている場合には、このメッセージは、ＴＭＳＩ又はＩＭＳＩについて１つ、及びＩＭＥＩについて１つ、合計で２つの移動端末装置識別情報（MOBILE IDENTITY information)を含まなければならない。位置更新要求メッセージがＩＭＥＩのみを含んでいる場合には、このメッセージは今日のシステムで使われている在来の位置更新要求メッセージと同一でなければならない。

【００３０】ＩＭＥＩ１５を得る方法とは無関係に、ＭＳＣ３０の明示の識別要求（IDENTITY REQUEST）シーケンスを介して又は自動的に位置更新要求（LOCATION UPDATING REQUEST)の好ましい強化メッセージ（preferred enhancement)又はその他の在来の必須メッセージを介して、ＭＳＣ３０は、図２のブロック３０５において、ＭＴ１０から通知されたＩＭＥＩ１５の状況を判定するためにＥＩＲ６０に照会を行う。ＩＭＥＩ１５が盗まれた移動電話として又はひどい故障のある装置として「ブラックリスト」に載っているとＥＩＲ６０が指摘したならば、ブロック３１０からブロック３１１へ移行して、ＭＳＣ３０はＭＴ－ＵＩＭロック機能が作動可能（イネーブル）になっているか否か判定する。ブロック３１０においてＥＩＲ６０の照会により移動端末装置が盗まれたり「ブラックリスト」に載っていたりしないことが分かったならば、ブロック３３５に移行してプロセスは終了する。

【００３１】ＭＴ－ＵＩＭロック機能は通常は作動可能にされるけれども、特定のＭＳＣ３０については、そのオペレータが希望する場合には、作動不能にされる。ブロック３１１でこの機能が作動可能であればブロック３１１での分岐は図３のブロック３１５へ移行する。もしＭＴ－ＵＩＭロック機能が作動不能になっていれば、ブロック３１１での分岐はブロック３２０へ移行する。

【００３２】ブロック３１５に至ると、ＭＳＣ３０は、ＭＴ－ＵＩＭロックコマンドを示す保障要求メッセージ（SECURITY REQUEST MESSAGE）（図７（Ａ））を作成して、図１に示されているＭＴ１０と通信中のＢＳＣ４０ユニット及びＢＴＳ５０ユニットを介してこのメッセージを送る。本発明の好ましい実施例では、全ての保障要求メッセージは暗号モードで送られる。

【００３３】ＭＴ－ＵＩＭロックコマンドを意味する保障要求メッセージ（SECURITY REQUEST MESSAGE）は、該コマンドは有効であって無許可のいたずらや「ハッキング（hacking)」の結果ではないことを保証する手段をＭＴ１０に与えるために、ユーザのＵＩＭ２０に関連するＨＬＲ３５のＡｕＣ３６の機能を介して提供されるＲＡＮＤ及びＳＲＥＳ（真実性確認パラメータ）の対を含んでいる。ブロック３１５からブロック３１６（図４及び図５参照）へ移行する。ブロック３１６で、ＭＳＣ３０はＭＴ１０からの応答を待つ。

【００３４】図４及び図５は、本発明に関連する移動端末装置ＭＴ１０の論理の概要を示す。ＭＳＣ３０からメッセージを受け取ると、ＭＴ１０は、受け取ったメッセージが新たに定義されたロックの１つを起動させるコマンドを表しているのか否かを判定しなければならない（ステップ１００）。ステップ１０５において、そのメッセージがＭＴ－ＵＩＭロックを意味する保障要求メッセージであるか否かを検査するチェックが第１の好まし

いチェックであるとされている。もしメッセージがそのようなコマンドを含んでいるならば、ステップ１０５からステップ１２０へ移行する。もしメッセージがMT－ＵＩＭロックでなければ、ステップ１０５からステップ１１０へ分岐する。

【００３５】移動端末装置ＭＴ１０のステップ１１０以降の処理について、図３のＵＩＭ－ＩＭＥＩロックのステップ３２５に関連するＭＳＣ３０の論理の後に、解説をする。

【００３６】図４のステップ１２０において、ＭＴ１０は、受け取ったメッセージが正当であるか否かを確かめなければならない。このことは、ＵＩＭ２０での在来の真実性確認手続きをＭＴ１０での新しい手続きと組み合わせて利用して該機能を実行することによって、行われる。図７（Ａ）に記されているように、ＭＴ－ＵＩＭロックメッセージは、当業者に周知されているＡｕＣ３６からのＲＡＮＤを含んでいる。この手続きを強化するために、本発明の好ましい実施例は、ハッキングからの保護のために追加の要件をＲＡＮＤに課す。それらの要件は、慎重に考慮されるべきであり、また特定の実施に特有のものでなければならない。好ましい強化方法は、ランダムに選ばれたＲＡＮＤを伴う真実性確認要求（AUTHENTICATION REQUEST）をＭＴ１０に作成させて、その要求をＭＳＣ３０に送らせることである。するとＭＳＣ３０は、ＭＴ１０から受け取ったＲＡＮＤを適切なＨＬＲ３５のＡｕＣ３６の機能に送り、正しいＳＲＥＳ応答を受け取る。ＭＳＣ３０は、その後、前記ＳＲＥＳを含む真実性確認応答メッセージ（AUTHENTICATION RESPONSE message)を作成してＭＴ１０に送る。するとＭＴ１０は、ＭＳＣ３０から受け取った真実性確認応答（AUTHENTICATION RESPONSE)の中のＳＲＥＳを、初めにＭＳＣ３０に真実性確認要求メッセージで送られたＲＡＮＤを用いてＵＩＭ２０が計算したＳＲＥＳと比較する。この２つのＳＲＥＳの値が一致すれば、保障要求は本物である（真実性がある）と考えられる。この方法は、当業者には容易に理解できる上記のメッセージ交換を支援するようにＭＳＣ３０とＡｕＣ３６とを改造することを必要とする。ここで考察している強化方法の他の実例は、前に受け取ったＲＡＮＤの充分な長さのリストを維持して、メッセージで受け取ったＲＡＮＤをこのリストと付き合わせて検査することである。維持されているリストの中にそのＲＡＮＤが見つかって、その様な一致の確率がありそうもないと人が考えたならば、そのメッセージを捨てることができ、ステップ１３１へ分岐をする。この種の手続きを、例えばＲＡＮＤを含む種々のメッセージを受け取る頻度を監視するなどの他の手続きと組み合わせることができる。けれども、追加の強化の方法を詳しく特定することは、与えるべきでない情報を「ハッカー」に与える結果を招くだけである。特定のＭＴ１０装置のために選ばれた好ましい強化方法をＲＡＮＤが承認すれば、ＭＴ１０は真実性確認プロセスを続行する。ＲＡＮＤは在来の手段を介してＵＩＭ２０に送られ、ＵＩＭ２０は、ＵＩＭ２０の真実性確認論理により在来の方法で計算されたＳＲＥＳ値を返す。ステップ１３０において、ＭＴ１０は、ＭＳＣ３０から受け取ったＭＴ－ＵＩＭロックメッセージの中のＳＲＥＳをＵＩＭ２０が計算したＳＲＥＳと比較する。その２つのＳＲＥＳの値が同一であるならば、ＭＴ－ＵＩＭロックコマンドは本物である（真実性がある）と見なされて正当なものとして承認され、次にステップ１３０からステップ１４０へ移行する。ステップ１３０で本物ではない（真実性がない）と判定されたならば、ステップ１３１へ移行する。

【００３７】ステップ１４０においてＭＴ１０は内面的なＵＩＭロック手続きを実行してＭＴ１０に現在装填されているＵＩＭ２０のカードのみを容認するようにＭＴ１０の処理を変更する。ＵＩＭロック手続きは当該ＭＴ１０のハードウェア及びソフトウェアのデザインに独特のものであり、「ハッキング」その他の不正行為からこの機能を確実に守るために、厳重に保護されなければならない。特定のＭＴ１０のためのＵＩＭロック手続きは当業者にはよく知られているけれども、特定のＭＴ１０のデザインへの適用は、それを開示すれば安全が損なわれる危険があるために、決して開示されない。ステップ１４０からステップ１４１へ移行し、ここでＭＴ１０はＭＴ－ＵＩＭロック手続きが成功したか否か判定する。もし成功であればステップ１４２へ、失敗であればステップ１３１へ分岐する。

【００３８】ステップ１４２においてＭＴ１０は、該ＭＴが当該ＵＩＭ２０にロックしていることを確認しており、従ってＭＴ－ＵＩＭロックが成功したことを意味する保障応答（SECURITY RESPONSE)（図７（Ｂ））を作成する。このメッセージはＭＳＣ３０に送られる。次にステップ１５０に移行してプロセスは終了する。

【００３９】ステップ１３１は、ＭＴ－ＵＩＭロック動作が失敗したこと、及びその失敗の理由を示す保障応答を作成する。このメッセージは、ＭＳＣ３０に送られて、失敗の理由が真実性がなかったこと（authentication failure）なのか或いはその他の処理の失敗であるのかを指摘する。次にステップ１５０に移行してプロセスは終了する。

【００４０】ＭＴ１０の制御の流れを詳細に検討したので、次に図３のステップ３１６を参照するが、そこではＭＣＳ３０の制御の流れに関する検討は行われていなかった。ＭＳＣ３０は、ＭＴ１０から応答を受け取るか又はＭＴ１０からの応答を処理すると、ステップ３１６からステップ３１７へ移行し、このステップでＭＳＣ３０は、将来ステップ３３０で参照するためにＭＴ１０からのＭＴ－ＵＩＭロック動作の結果に関する情報を記憶する。次にステップ３１７からステップ３２０へ移行する。

【００４１】ブロック３２０でＭＳＣ３０はＵＩＭ－ＩＭＥＩロック機能が作動可能（イネーブル）になっているか否か判定する。この機能が作動可能であるか否か判定するための条件は、取り締まり問題やオペレータの好みやその他の要素に依存して大いに多様であり、従ってこの機能については「標準」動作モードは期待できなくて、全くオペレータの好みによる。しかし、この機能が動作可能であるならば、制御の流れはブロック３２０からブロック３２５へ分岐する。この機能が作動不能になっているならば制御の流れはブロック３２０からブロック３３０へ分岐する。

【００４２】ブロック３２５において、ＭＳＣ３０は、ＵＩＭ－ＩＭＥＩロックコマンドを意味する保障要求を作成して、このメッセージをＭＴ１０へ送る。ＭＴ－ＵＩＭロックコマンドと同じく、ＵＩＭ－ＩＭＥＩロックコマンドは、ＵＩＭ２０に付随するＡｕＣ３６の機能からのＲＡＮＤ及びＳＲＥＳ（真実性確認パラメータ）の対を、動作が本物である（真実性がある）ことを証明するための手段として含んでいる。ブロック３２５からブロック３３０へ移行する。

【００４３】ＭＳＣ３０の制御はステップ３２５からステップ３２６（図４及び図５参照）へ移行し、ここでＭＳＣ３０は実際上、応答を待つか、或いはＭＴ１０のための応答を待ちながら時間切れとなるので、今や図４及び図５に示されているＭＴ１０の処理に焦点を合わせる。

【００４４】前述したように、ＭＴ１０がＭＳＣ３０からメッセージを受け取ると、ステップ１００から１０５までの制御が行われる。もしステップ１０５において、受け取られたメッセージがＭＴ－ＵＩＭロックコマンドを意味するものでなかったならば、ステップ１０５からステップ１１０へ移行する。

【００４５】ステップ１１０は、受け取ったメッセージの内容を検査して、それがＵＩＭ－ＩＭＥＩロックコマンドを含んでいるか否か判定する。もし含んでいるならば、ステップ１１０からステップ１２５へ分岐する。もし含んでいなければ、ステップ１１０からステップ１１５へ分岐する。

【００４６】ステップ１１５は、本発明には関係のないＭＳＣ３０から受け取られた他のコマンドの処理を表しており、従って本発明の範囲内での処理は終了したと考えてよい。

【００４７】ステップ１２５は、受け取られたＵＩＭ－ＩＭＥＩロックコマンドが本物である（真実性がある）ことを保証するためのものである。図７（Ａ）に示されているように、ＵＩＭ－ＩＭＥＩロックコマンドを意味する保障要求は、当該ＵＩＭ２０に付随するＡｕＣ３６により該ＵＩＭ２０のために計算されたＲＡＮＤ及びＳＲＥＳを含んでいる。図４のステップ１２０に関して前述したように、好ましい実施例では、ＭＴ１０によりＲ

ＡＮＤに追加の強化要件が課される。それらの強化要件は実施者の決定により、ステップ１２０で選ばれたものと意図的に異ならしめることもできるし、同一であってもよい。もし強化されたＲＡＮＤ要件が承認されなければ、ＭＴ１０はステップ１３５でそのコマンドは無効であると宣言してステップ１３６へ分岐する。そうでない場合にはＵＩＭ－ＩＭＥＩロックコマンドはＭＴ１０からＵＩＭ２０に渡され、更なる処理のためにＭＳＣ３０から受け取られたメッセージに含まれるＲＡＮＤ及びＳＲＥＳの両方を完備している。次にステップ１３５からステップ１４５へ移行する。

【００４８】ステップ１４５において、ＭＴ１０はＵＩＭ－ＩＭＥＩロックメッセージをＵＩＭ２０に送り、動作の結果又は時間切れを待つ。

【００４９】図６は、ＵＩＭ－ＩＭＥＩロックコマンドの処理のためのＵＩＭ２０内での制御の流れを示す。ＭＴ１０のステップ１４５からのＵＩＭ－ＩＭＥＩロックコマンドの受け取りでプロセスが始まり、その結果として図６のＵＩＭ２０のステップ２００となる。ステップ２００からステップ２０５へ移行して、このステップでＵＩＭは、ＵＩＭ－ＩＭＥＩロックメッセージに含まれているＲＡＮＤを抽出して、通常の方法でＳＲＥＳを計算する。ステップ２０５でＵＩＭ２０がＳＲＥＳを計算した後、ステップ２１０へ移行し、ここでＵＩＭ２０により計算されたＳＲＥＳと、ＭＳＣ３０からのＵＩＭ－ＩＭＥＩロックメッセージに含まれているＳＲＥＳとが比較される。その２つのＳＲＥＳの値が同一であれば、ステップ２１０からステップ２１５へ分岐する。その２つのＳＲＥＳの値が同一でなければ、ステップ２１０からステップ２３０へ移行する。

【００５０】ステップ２１５においてＵＩＭ２０はＭＴ１０からＩＭＥＩ１５を要求する。ＩＭＥＩ１５の値は、将来、各初期化サイクルなどの際に参照するためにＵＩＭ２０に記憶される。ステップ２１５からステップ２２０へ移行し、ここでステップ２１５の成功が検査される。もし動作が首尾よく終了すれば、ステップ２２０からステップ２２５へ移行する。もしそうでなければ、ステップ２２０からステップ２３０へ分岐する。

【００５１】ステップ２２５は、ＵＩＭが今や首尾よく特定のＩＭＥＩ１５にロックされているという事実のインジケータをＵＩＭ２０に記憶させることにより、その事実を記憶する。また、ＵＩＭ２０は、ＵＩＭ－ＩＭＥＩロックコマンドが首尾よく実行されたことをＭＴ１０に知らせる。ステップ２２５からステップ２３５へ移行してプロセスは終了する。

【００５２】ステップ２３０は、ステップ１４５のＵＩＭ－ＩＭＥＩロック動作の実行（又は時間切れ）の知らせをＭＴ１０に送り、ステップ１４６に進み、ここでもし動作が成功であったならば、ＭＴ１０はステップ１４６からステップ１４７へ分岐する。もしそうでなけれ

ば、ステップ１４６からステップ１３６へ分岐する。

【００５３】ステップ１４７において、ＭＴ１０は、ＵＩＭ－ＩＭＥＩロックが成功したことを意味する保障応答（SECURITY RESPONSE)を作成して、このメッセージをＭＳＣ３０に送る。ＭＴ１０の制御はステップ１４７からステップ１５０へ移行し、ＭＴ１０のプロセスは終了する。

【００５４】ステップ１３６においてＭＴ１０はＵＩＭ－ＩＭＥＩロックの失敗を意味する保障応答を作成して、このメッセージをＭＳＣ３０に送る。次にＭＴ１０の制御はステップ１３６からステップ１５０に移行し、ＭＴ１０のプロセスは終了する。

【００５５】ここで図３を参照すると、ＭＳＣ３０がＭＴ１０から応答を受け取るとステップ３２６からの制御の流れはステップ３２７へ進む。ステップ３２７においてＭＳＣ３０は、ステップ３３０での参照のためにＭＴ１０から通知された結果を記憶する。次にステップ３２７からステップ３３０へ移行する。

【００５６】ブロック３３０は管理に関する報告の処理をする。好ましい実施例では、その報告には、当該ＭＴ１０のＩＭＥＩ１５、ＥＩＲ６０からのＩＭＥＩ１５に関連する状況、ＭＴ１０に内蔵されているＵＩＭ２０に関連するユーザーと、ＭＳＣ３０がとった行動とに関する情報と（これには、分岐の仕方により、報告のみ（Report Only)、ＭＴ－ＵＩＭロック（成功／失敗／試行されず）、ＵＩＭ－ＩＭＥＩロック（成功／失敗／試行されず）を含むことがある）、該当する場合にはＭＴ１０のロック動作の結果とが含まれる。これらの報告は、結局、将来行われるかも知れない犯罪調査等のために当該当局に送られる。

【００５７】ここで図８を参照すると、ステップ６０５において、ＵＩＭ２０は現在のＭＴ１０のＩＭＥＩ１５を要求する。ステップ６０５からステップ６１０へ移行し、ここでステップ６０５のＩＭＥＩ照会動作の成功が検査される。現在のＭＴ１０のＩＭＥＩ１５が受け取られると、ステップ６１０からステップ６１５へ分岐する。そうでない場合にはステップ６０５からステップ６２５へ分岐する。

【００５８】ステップ６１５は、現在のＭＴ１０から受け取られたＩＭＥＩ１５と、図６のステップ２１５においてＵＩＭ２０に記憶されたＩＭＥＩ１５とを比較する。もしその２つのＩＭＥＩの値が同一であれば、ステップ６２０からステップ６９９へ移行し、ここで通常の処理が続行され、本発明に関するプロセスは終了する。もしその２つのＩＭＥＩの値が同一でなければ、ステップ６２０からステップ６２５へ分岐する。

【００５９】ステップ６２５において、ＵＩＭ２０は現在のＭＴ１０から受け取ったＩＭＥＩ１５とは異なるＩＭＥＩ１５に現在ロックされているために初期化プロセスが止められていることをＭＴ１０に知らせる。次にステップ６２５からステップ６３０へ移行してプロセスは終了する。

【００６０】図７（Ａ）は、ＭＳＣ３０からＭＴ１０への保障要求メッセージの好ましい実施例である。このメッセージは新しいものであるが、このメッセージの幾つかの構成要素は既存のシステムに普通に使われているものである。新しい情報要素は保障要求メッセージタイプであり、これはメッセージのモビリティ管理セットの中でのこのメッセージタイプを一義的に特定する８ビットの値である。この値は標準化機構により割り当てられるものであり、モビリティ管理メッセージタイプの保障メッセージ範囲内で唯一無二の値であればどのような値でもよい。次の新しい情報要素は保障要求のタイプである。この情報要素の好ましい長さは８ビットである。１ビットは留保される。１ビットは要求されたロック状態を示すために使われ、０は「ロック解除」を意味し、１は「ロック」を意味する。１ビットは、ＭＴ－ＵＩＭロックを示し、１ビットはＵＩＭ－ＩＭＥＩロックを示す。残りは留保される。ＭＳＣ３０が１つのメッセージを介してＭＴ１０にロック動作をすること又は両ロックをロック解除することを指令するように、このＭＴ－ＵＩＭビット及びＵＩＭ－ＩＭＥＩビットをビットマスクとして使用することができる。しかし、好ましい実施例は、簡単のために、メッセージ毎に１回のロックだけである。本発明を実施するために他の多くのフォーマット及び構造を採用することができる。

【００６１】図７（Ｂ）はＭＴ１０からＭＳＣ３０への保障応答の好ましい実施例である。図７（Ａ）に記されているように幾つかの情報要素は従来から使われているものである。保障応答メッセージタイプは、メッセージのモビリティ管理セットの中でのこのメッセージタイプを一義的に特定する８ビットの値である。この値は標準化機構により割り当てられるものであり、モビリティ管理メッセージタイプの保障メッセージ範囲内で唯一無二の値であればどのような値でもよい。保障要求のタイプは図７（Ａ）に記載されているとおりである。簡単のために、好ましい実施例はメッセージ毎に１回のロック動作だけである。しかし、保障応答メッセージ中に２個以上のロック識別子セットがあるならば、各ロック識別子セットにつき１個ずつ、合計で複数の結果コード情報要素があることになる（即ち、値１）。結果コードは、第１結果コードＩＥＩがロッキングビットマップの最下位ビットで特定されるロック等に対応することとなるようにマッピングする。「０」という値は動作が成功したことを意味する。「１」という結果コードの値は、ＵＩＭ２０により計算されたＳＲＥＳが保障要求の中のＳＲＥＳと一致しなかったので失敗であったことを意味する。「１０」という２進法の結果コードは真実性の確認要求メッセージをＭＳＣ３０に送る好ましい強化方法の時間切れ失敗により動作が失敗したことを意味する。「１

1」という２進法の結果コードは、ＭＳＣ３０からの真実性の確認応答のＳＲＥＳが正しくなかったことを意味する。他の全ての値は種々のタイプの失敗を表し、その意味を知っているのは当該ＭＴ１０の製造者だけである。本発明を実施するために他の多くのフォーマット及び構造を採用することができる。

【００６２】図８は、本発明のＵＩＭ－ＩＭＥＩロックを実現するために在来の論理より前に挿入しなければならないＵＩＭ２０の論理を示す。ステップ６００において、ＵＩＭ２０の従来から行われている種類の処理の際になるべく早く、且つＵＩＭ２０の初期化が完了する前に、ＵＩＭ２０はその制御構造をチェックして、現在ＵＩＭ２０が特定のＭＴ１０に付随する特定のＩＭＥＩ１５にロックされているか否か判定する。もしそうであれば、ステップ６００からステップ６０５へ分岐する。もしそうでなければ、ステップ６００からステップ６９９へ分岐して、ここで従来から行われている種類の処理が続行され、本発明に関連する処理は終了する。

【００６３】移動端末装置ＭＴ１０の初期化処理のための類似の形を設けることができるけれども、ＭＴ１０からＵＩＭ２０へのロッキングは現在は種々の起動方法を介して行われているので、この情報は当業者に周知されていて、ここでは説明しない。

【００６４】メッセージを介してＭＴ－ＵＩＭ機能及びＵＩＭ－ＩＭＥＩ機能の両方のロック解除を支援することも本発明の目的である。当業者のために、保障要求メッセージのフォーマットは、図７（Ａ）に関して説明した「ロック解除」ビットを介してこれを支援する。ロック解除動作のための論理及び制御の流れは図４乃至図６を考察すれば明かである。ＭＳＣ３０についての論理的ロック解除動作は、トリガーを除けば図２及び図３のロック動作と全く同じである。ステップ３１０は、以前はブラックリストに載せられていたＭＴ１０のホワイトリストへの記入、又は適当なロック解除コマンドを強制的に送らせるためのオペレータの専門技術者及び種々のＭＳＣ３０インターフェースを介しての手操作による対話であってもよい。好ましい実施例は、「ブラックリスト」から「ホワイトリスト」への「バッチ」型転載処理と手操作による介在との両方を支援する。

【００６５】本発明の好ましい実施例を詳しく開示したけれども、明細書に記載し特許請求の範囲の欄において定義した発明の範囲から逸脱せずに、説明をした実施例について種々の変更がされ得ることを当業者は理解するべきである。

【図面の簡単な説明】

【図１】本発明の通信網の１実施例を示す略ブロック図である。

【図２】本発明の方法によるメッセージの処理のための通信網論理（図１のＭＳＣ３０）のフローチャート（その１）である。

【図３】本発明の方法によるメッセージの処理のための通信網論理（図１のＭＳＣ３０）のフローチャート（その２）である。

【図４】本発明の方法によるメッセージの処理のための移動端末装置論理（図１のＭＴ１０）のフローチャート（その１）である。

【図５】本発明の方法によるメッセージの処理のための移動端末装置論理（図１のＭＴ１０）のフローチャート（その２）である。

【図６】本発明で取り入れたメッセージの処理のためのユーザー識別モジュール論理（図１のＵＩＭ２０）のフローチャートである。

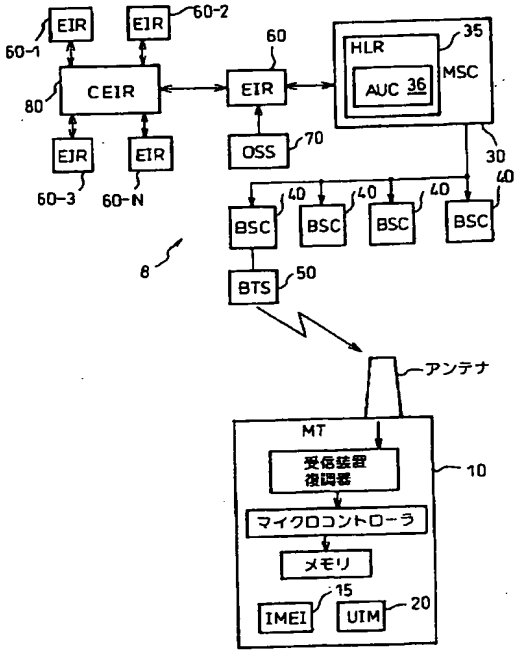
【図７】（Ａ）および（Ｂ）はそれぞれ、本発明に用いることのできるメッセージの構成を示す。

【図８】本発明の実施例におけるＵＩＭ－ＩＭＥＩロックを実行するために図１のＵＩＭ２０において必要とされる初期化論理についてのフローチャートである。

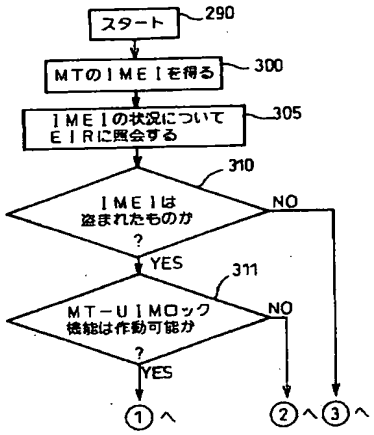
【符号の説明】

ＭＴ…移動端末装置
ＵＩＭ…ユーザー識別モジュール
ＩＭＥＩ…国際移動端末装置識別ユニット
ＭＳＣ…移動交換センター
ＢＳＣ…基地局コントローラ

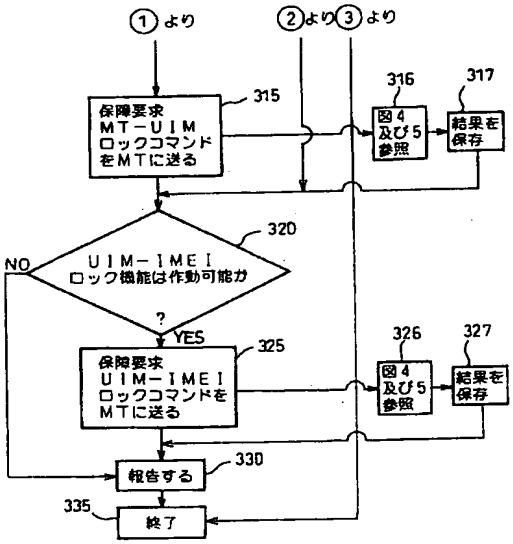
【図1】


EIR
EIR
60-2
60-1
60
HLR
35
CEIR
EIR
MSC
AUC 36
80
EIR
EIR
OSS
70
30
60-3
60-N
40
BSC
BSC
BSC
BSC
8
BTS
50
アンテナ
MT
受信装置
復調器
10
マイクロコントローラ
メモリ
15
IMEI
UIM
20

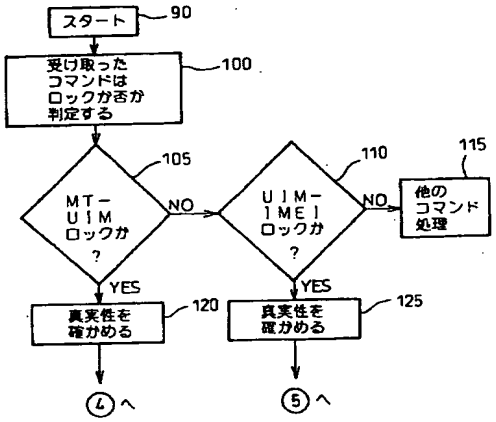
【図2】


スタート
290
MTのIMEIを得る
300
IMEIの状況について
EIRに照会する
305
310
IMEIは
盗まれたものか
NO
YES
311
MT－UIMロック
機能は作動可能か
NO
YES
①へ
②へ③へ

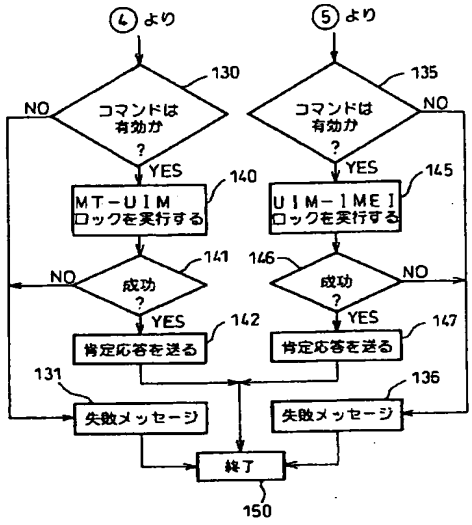
【図3】


①より
②より③より
保障要求
MT－UIM
ロックコマンド
をMTに送る
315
316
図4
及び5
参照
317
結果を
保存
320
NO
UIM－IMEI
ロック機能は作動可能か
?
YES
保障要求
UIM－IMEI
ロックコマンドを
MTに送る
325
326
図4
及び5
参照
327
結果を
保存
報告する
330
335
終了

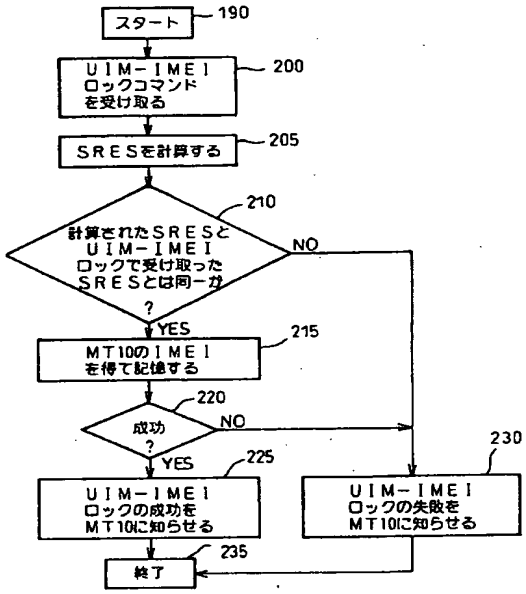
【図4】


スタート
90
受け取った
コマンドは
ロックか否か
判定する
100
105
MT－
UIM
ロックか
?
NO
110
UIM－
IMEI
ロックか
?
NO
115
他の
コマンド
処理
YES
YES
真実性を
確かめる
120
真実性を
確かめる
125
④へ
⑤へ

【図5】



【図6】



【図7】

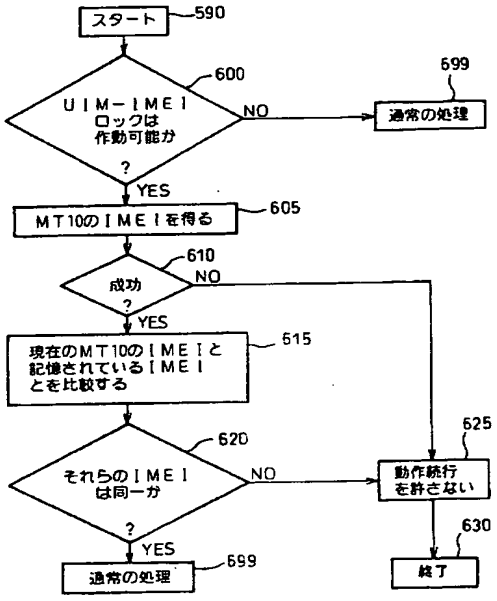
(A) 保障要求

モビリティ管理プロトコルディスクリミネータ
スキップインジケータ
保障要求メッセージタイプ
保障信号のタイプ
真実性パラメータRAND
真実性パラメータSRES

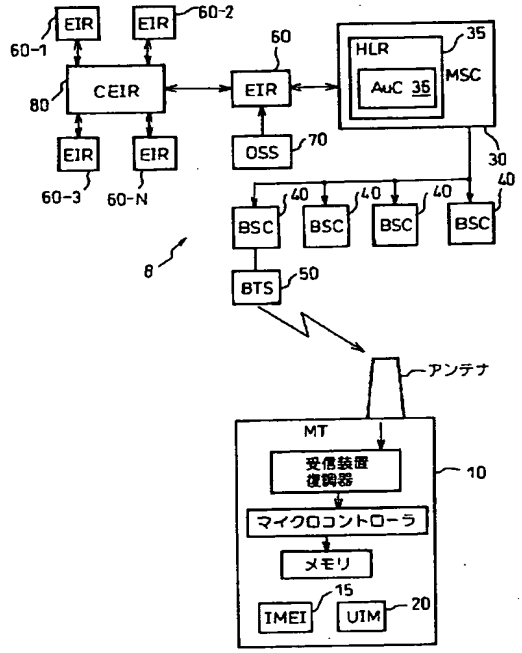
(B) 保障応答

モビリティ管理プロトコルディスクリミネータ
スキップインジケータ
保障応答メッセージタイプ
保障要求のタイプ
結果コード

【図8】



【手続補正書】
【提出日】平成８年８月１４日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項９
【補正方法】変更
【補正内容】
【請求項９】　前記移動交換センター（ＭＳＣ）は、真実性の確認センター（ＡｕＣ）を有するホームロケーション・レジスタ（ＨＬＲ）を含んでおり、前記移動交換センター（ＭＳＣ）は、前記移動端末装置の正当性及び状況に関するデータを内蔵する装置識別レジスタ（ＥＩＲ）に接続されている、請求項８に記載の移動通信網。
【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図１
【補正方法】変更
【補正内容】
【図１】



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.